What is claimed is:

1. A method of generating a keystream, comprising the steps of:

providing data bits from predetermined register stages of multiple feedback shift registers to a first randomization stage, each feedback shift register having input, intermediate, and output stages through which the data bits are shifted serially in response to a clock signal;

providing output of said first randomization stage to a second randomization stage;

providing output of said second randomization stage and data bits from other predetermined register stages of said feedback shift registers to at least one additional randomization stage, wherein,

said data bits are permutated at each randomization stage and output of a final randomization stage provides said keystream.

2. A method in accordance with claim 1, wherein a third randomization stage is the final randomization stage.

3. A method in accordance with claim 1, further comprising the step of:

varying at least one feedback shift register structure in response to a polynomial code signal generated by a polynomial code signal generator.

4. A method in accordance with claim 3, further comprising the step of:

varying the polynomial code used to generate the polynomial code signal.

5. A method in accordance with claim 1, wherein the feedback shift registers comprise:

a plurality of dynamic feedback shift registers; and

at least one static feedback shift register.

6. A method in accordance with claim 1, wherein the feedback shift registers comprise:

a first dynamic feedback shift register;

a second dynamic feedback shift register; and

a static feedback shift register.

7. A method in accordance with claim 6, further comprising the steps of:

inputting seed data into an input buffer;

providing a first portion of the seed data from the input buffer to the first dynamic feedback shift register;

providing a second portion of the seed data from the input buffer to the second dynamic feedback shift register; and

providing a third portion of the seed data from the input buffer to the static feedback shift register.

8. A method in accordance with claim 7, wherein:

the data bits of the dynamic feedback shift registers are shifted serially from each register stage in response to a clock signal;

a number of finite field adders are arranged between predetermined pairs of the register stages of the dynamic feedback shift registers, such that one of the inputs to each adder is provided from the preceding register stage and the other input of each adder is fed back from the output terminal of the output stage via a finite field multiplier.

9. A method in accordance with claim 1, wherein the first randomization stage comprises a randomization table for permuting data bits from predetermined register stages.

10. A method in accordance with claim 1, wherein the second randomization stage comprises a non-linear mixing function to combine the output of said second randomization stage and data bits from other

predetermined register stages of said feedback shift registers.

11. A method in accordance with claim 1, wherein the third randomization stage comprises multiple non-linear S-Boxes.

12. A method in accordance with claim 11, wherein the S-Boxes are 8*8 S-Boxes.

13. A method in accordance with claim 1, wherein the third randomization stage comprises 256 non-linear 8*8 S-Boxes.

14. A method in accordance with claim 1, wherein the feedback shift registers are constructed using an extended Galois field ($GF(2^m)$).

15. A method in accordance with claim 14, wherein m equals eight.

16. A method in accordance with claim 14, wherein the polynomials used for the feedback shift registers are primitive and irreducible.

17. A method in accordance with claim 1, wherein the first randomization stage comprises multiple

randomization tables for permuting data bits from predetermined register stages.

18. A method in accordance with claim 17, wherein the multiple randomization tables comprise eight randomization tables.

19. A method in accordance with claim 1, further comprising the step of:

multiplexing the data bits from the feedback shift registers prior to input into the first randomization stage.

20. A method in accordance with claim 1, further comprising the steps of;

providing the output from the third randomization stage to a pre-keystream register;

providing alternate bits of the output from said pre-keystream register to a select chain buffer;

providing output from the select chain buffer to a decoding logic unit, which decoding logic unit decodes a particular polynomial for use in generating a polynomial code signal, said polynomial code signal being provided to at least one feedback shift register; and

providing the remaining bits of the output from said pre-keystream register to a keystream register,

wherein the output of the keystream register provides said keystream.

21. A method in accordance with claim 20, wherein the third randomization stage comprises multiple non-linear S-Boxes.

22. A method in accordance with claim 21, further comprising the steps of:

providing certain output of the S-Boxes to a codestream register;

clocking said output through said codestream register;

adding said output to data bits shifted from at least one of the feedback shift registers via a non-binary adder to produce feedback data bits;

providing the feedback data bits to the input stage and predetermined intermediate stages of at least one of the feedback shift registers.

23. A method in accordance with claim 1, wherein:

a 192 bit shared seed input key is provided to the multiple feedback shift registers; and

a 56 bit keystream output is generated.

24. A method in accordance with claim 23, wherein the 192 bit shared seed input key is derived from a 128 bit input by duplicating half the bits.

25. A keystream generator apparatus, comprising:

multiple feedback shift registers, each feedback shift register having input, intermediate, and output stages through which data bits are shifted serially in response to a clock signal;

a first randomization stage which receives output from predetermined register stages of the multiple feedback shift registers;

a second randomization stage which receives output from said first randomization stage;

a third randomization stage which receives output from said second randomization stage and data bits from other predetermined register stages of said feedback shift registers, wherein,

said data bits are permutated at each randomization stage and output of a final randomization stage provides said keystream.

26. Apparatus in accordance with claim 25, wherein the third randomization stage is the final randomization stage.

27. Apparatus in accordance with claim 25, wherein:

at least one feedback shift register structure is varied in response to a polynomial code signal generated by a polynomial code signal generator.

28. Apparatus in accordance with claim 27, wherein:

the polynomial code used to generate the polynomial code signal is varied.

29. Apparatus in accordance with claim 25, wherein the feedback shift registers comprise:

a plurality of dynamic feedback shift registers; and

at least one static feedback shift register.

30. Apparatus in accordance with claim 25, wherein the feedback shift registers comprise:

a first dynamic feedback shift register;

a second dynamic feedback shift register; and

a static feedback shift register.

31. Apparatus in accordance with claim 30, wherein:

seed data is input into an input buffer;

a first portion of the seed data from the input buffer is provided to the first dynamic feedback shift register;

a second portion of the seed data from the input buffer is provided to the second dynamic feedback shift register; and

a third portion of the seed data from the input buffer is provided to the static feedback shift register.

32. Apparatus in accordance with claim 31, wherein:

the data bits of the dynamic feedback shift registers are shifted serially from each register stage in response to a clock signal;

a number of finite field adders are arranged between predetermined pairs of the register stages of the dynamic feedback shift registers, such that one of the inputs to each adder is provided from the preceding register stage and the other input of each adder is fed back from the output terminal of the output stage via a finite field multiplier.

33. Apparatus in accordance with claim 25, wherein the first randomization stage comprises a randomization table for permuting data bits from predetermined register stages.

34. Apparatus in accordance with claim 25, wherein the second randomization stage comprises a non-linear mixing function to combine the output of said second

randomization stage and data bits from other predetermined register stages of said feedback shift registers.

35. Apparatus in accordance with claim 25, wherein the third randomization stage comprises multiple non-linear S-Boxes.

36. Apparatus in accordance with claim 35, wherein the S-Boxes are 8*8 S-Boxes.

37. Apparatus in accordance with claim 25, wherein the third randomization stage comprises 256 non-linear 8*8 S-Boxes.

38. Apparatus in accordance with claim 25, wherein the feedback shift registers are constructed using an extended Galois field ($GF(2^m)$).

39. Apparatus in accordance with claim 38, wherein m equals eight.

40. Apparatus in accordance with claim 38, wherein the polynomials used for the feedback shift registers are primitive and irreducible.

41. Apparatus in accordance with claim 25, wherein the first randomization stage comprises multiple randomization tables for permuting data bits from predetermined register stages.

42. Apparatus in accordance with claim 41, wherein the multiple randomization tables comprise eight randomization tables.

43. Apparatus in accordance with claim 25, wherein:

the data bits from the feedback shift registers are multiplexed prior to input into the first randomization stage.

44. Apparatus in accordance with claim 25, further comprising;

a pre-keystream register for receiving the output from the third randomization stage;

a select chain buffer for receiving alternate bits of the output from said pre-keystream register;

a decoding logic unit for receiving output from the select chain buffer, which decoding logic unit decodes a particular polynomial for use in generating a polynomial code signal, said polynomial code signal being provided to at least one feedback shift register; and

a keystream register for receiving the remaining bits of the output from said pre-keystream register, wherein output of the keystream register provides said keystream.

45. Apparatus in accordance with claim 44, wherein the third randomization stage comprises multiple non-linear S-Boxes.

46. Apparatus in accordance with claim 45, wherein:

certain output of the S-Boxes is provided to a codestream register;

said output is clocked through said codestream register;

said output is added to data bits shifted from at least one of the feedback shift registers via a non-binary adder to produce feedback data bits; and

said feedback data bits are provided to the input stage and predetermined intermediate stages of at least one of the feedback shift registers.

47. Apparatus in accordance with claim 25, wherein:

a 192 bit shared seed input key is provided to the multiple feedback shift registers; and

a 56 bit keystream output is generated.

48. Apparatus in accordance with claim 25, wherein the 192 bit shared seed input key is derived from a 128 bit input by duplicating half the bits.